

Data Processing Agreement

pursuant to Article 28(3) of Regulation 2016/679 (GDPR) for the purpose of the data processor's processing of personal data

Data Processing Agreement prepared on the basis of the Danish Data Protection Agency's standard contractual clauses approved by the European Data Protection Board

Last updated on 01.04.2026

between

GENERIC DATA CONTROLLER
GENERIC ADDRESS
DK
CVR no.:

hereinafter "the Data Controller"

and

BOARD OFFICE A/S
Jernbanegade 14
9000 Aalborg
DK
CVR no.: 28966237

hereinafter "the Data Processor"

---

each a "Party"; together "the Parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights and freedoms of natural persons and the protection of their privacy.

Contents

1.	Preamble	04
2.	The rights and obligations of the Data Controller	04
3.	The Data Processor acts according to instructions	05
4.	Confidentiality	05
5.	Security of processing	05
6.	Use of sub-processors	06
7.	Transfer of data to third countries or international organisations	07
8.	Assistance to the Data Controller	07
9.	Notification of personal data breach	09
10.	Erasure and return of data	09
11.	Audit and inspection	09
12.	The Parties' agreement on other terms	10
13.	Commencement and termination	10
14.	Contact persons of the Data Controller and the Data Processor	10

Appendices

Appendix A	Information about the processing	11
Appendix B	Sub-processors	13
Appendix C	Instruction pertaining to the processing of personal data	14
Appendix D	The Parties' terms of agreement on other subjects	22
Appendix E	Processing of personal data when using BOARD Assistant™	23

1. Preamble

1.1 These Clauses set out the rights and obligations of the Data Processor when processing personal data on behalf of the Data Controller.

1.2 The Clauses have been designed to ensure the Parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR").

1.3 In the context of the provision of BOARD-OFFICE & BOARD-PEOPLE, the Data Processor will process personal data on behalf of the Data Controller in accordance with these Clauses.

1.4 The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.

1.5 Appendices are attached to these Clauses, and the Appendices form an integral part of the Clauses.

1.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

1.7 Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.

1.8 Appendix C contains the Data Controller's instructions with regard to the Data Processor's processing of personal data, the minimum security measures to be implemented by the Data Processor and how audits of the data processor and any sub-processors are to be performed.

1.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

1.10 Where standard contractual clauses as referred to in Article 46(1)(c) and (d) GDPR form the basis for transfers of personal data between the Data Controller and the Data Processor to third countries as referred to in Chapter V GDPR, these are attached in their English version as Appendix E and E1.

1.11 The Clauses along with their appendices shall be retained in writing, including electronically, by both Parties.

1.12 These Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.

2. The rights and obligations of the Data Controller

2.1 The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable data protection provisions of other EU law or the national law of the EU/EEA Member States and these Clauses.

2.2 The Data Controller has the right and obligation to decide for which purpose(s) and by which means personal data may be processed.

2.3 The Data Controller shall be responsible, among other things, for ensuring that the processing of personal data which the Data Processor is instructed to perform has a legal basis.

3. The Data Processor acts according to instructions

3.1 The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by EU law or the national law of the EU/EEA Member States to which the Data Processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with these Clauses.

3.2 The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, an instruction infringes the GDPR or the applicable data protection provisions of other EU law or the national law of the EU/EEA Member States.

4. Confidentiality

4.1 The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn if access is no longer necessary, and personal data shall consequently no longer be accessible to those persons.

4.2 The Data Processor shall at the request of the Data Controller demonstrate that the persons concerned under the Data Processor's authority are subject to the above-mentioned confidentiality.

5. Security of processing

5.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

5.1.1 Pseudonymisation and encryption of personal data

5.1.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services

5.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 According to Article 32 GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

5.3 Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Article 32 GDPR by, inter alia, providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR.

If – in the assessment of the Data Controller – mitigation of the identified risks requires further measures to be implemented than those already implemented by the Data Processor, the Data Controller shall specify the additional measures to be implemented in Appendix C.

6. Use of sub-processors

6.1 The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

6.2 The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of these Clauses without the prior general written authorisation of the Data Controller.

6.3 The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 30 calendar days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Data Controller can be found in Appendix B.

6.4 Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in these Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU law or the national law of the EU/EEA Member States, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the GDPR.

The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to these Clauses and the GDPR.

6.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in these Clauses are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data

protection content of the sub-processor agreement shall not require submission to the Data Controller.

6.6 In its agreement with the sub-processor, the Data Processor shall include the Data Controller as a third-party beneficiary, so that the Data Controller – in the event that the Data Processor has factually or legally ceased to exist, or in the event of the Data Processor's bankruptcy – has the right to terminate the sub-processor agreement and to instruct the sub-processor to delete or return the personal data.

6.7 If the sub-processor does not fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

7.1 Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

7.2 In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, are required under EU law or the national law of the EU/EEA Member States to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.3 Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of these Clauses:

7.3.1 transfer personal data to a data controller or a data processor in a third country or in an international organisation

7.3.2 transfer the processing of personal data to a sub-processor in a third country

7.3.3 process the personal data in a third country

7.4 The Data Controller's instructions regarding the transfer of personal data to a third country, including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

7.5 These Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and these Clauses cannot be relied upon by the Parties as a transfer tool under Chapter V GDPR unless such standard contractual clauses are attached as Appendix E.

8. Assistance to the Data Controller

8.1 Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of

the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

8.1.1 the right to be informed when collecting personal data from the data subject

8.1.2 the right to be informed when personal data have not been obtained from the data subject

8.1.3 the right of access by the data subject

8.1.4 the right to rectification

8.1.5 the right to erasure ("the right to be forgotten")

8.1.6 the right to restriction of processing

8.1.7 the notification obligation regarding rectification or erasure of personal data or restriction of processing

8.1.8 the right to data portability

8.1.9 the right to object

8.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

8.2 In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 5.3, the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

8.2.1 the Data Controller's obligation to, without undue delay and where feasible not later than 72 hours after having become aware of it, notify the personal data breach to the Danish Data Protection Agency (Datatilsynet), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

8.2.2 the Data Controller's obligation to, without undue delay, communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons

8.2.3 the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment) prior to the processing

8.2.4 the Data Controller's obligation to consult the Danish Data Protection Agency (Datatilsynet), where competent, prior to processing if a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

8.3 The Parties shall define in Appendix C the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clauses 8.1 and 8.2.

9. Notification of personal data breach

9.1 The Data Processor shall notify the Data Controller without undue delay after becoming aware that a personal data breach has occurred.

9.2 The Data Processor's notification to the Data Controller shall, if possible, take place immediately and no later than 48 hours after the Data Processor has become aware of the personal data breach, to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

9.3 In accordance with Clause 8.2.1, the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the Data Controller's notification to the competent supervisory authority:

9.3.1 the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

9.3.2 the likely consequences of the personal data breach

9.3.3 the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.4 The Parties shall define in Appendix D the information to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

10.1 On termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data and delete existing copies, unless EU law or the national law of the EU/EEA Member States requires storage of the personal data.

11. Audit and inspection

11.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and these Clauses and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

11.2 Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and sub-processors are specified in Appendices C.7 and C.8.

11.3 The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

12. The Parties' agreement on other terms

12.1 The Parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as such other clauses do not directly or indirectly contradict the Clauses or prejudice the fundamental rights and freedoms of the data subject afforded by the GDPR.

13. Commencement and termination

13.1 The Clauses shall become effective on the date of both Parties' signature.

13.2 Either Party may require the Clauses to be renegotiated if changes to the law or inexpediencies in the Clauses give rise to this.

13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other clauses governing the provision of personal data processing services have been agreed between the Parties.

13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 10.1 and Appendix C.4, the Clauses may be terminated by written notice by either Party.

13.5 Signature:

On behalf of the Data Controller

_____

On behalf of the Data Processor

_____

14. Contact persons of the Data Controller and the Data Processor

14.1 The Parties may contact each other via the contact persons below.

14.2 The Parties shall be under obligation continuously to inform each other of changes regarding contact persons.

Contact details for the Data Controller:
GENERIC NAME
GENERIC EMAIL/PHONE NUMBER

Contact details for the Data Processor:
Niels Arnold Lund, nal@board-office.dk

Appendix A Information about the processing

1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller

1.1 The following purposes form the basis of the Data Processor's processing of personal data on behalf of the Data Controller:

The data controller wishes to use the Data Processor's board portal BOARD-OFFICE, which is an online portal containing document storage, a discussion forum, a planning tool, digital signature, board job listings and an inspiration area.

In addition, the Data Processor is responsible for the operation, testing, maintenance, development and debugging of the Data Processor's applications.

2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing)

2.1 The Data Processor processes the Personal Data in connection with the Data Processor's provision of the board portals BOARD-OFFICE & BOARD-PEOPLE.

3. The processing includes the following types of personal data about data subjects

3.1 Name, address, telephone number, e-mail, user name for one or more systems, password for one or more systems, varying personal data provided or registered by the customer or the customer's customers without the organisation actively processing or identifying such data

BOARD OFFICE
In connection with the use of the BOARD OFFICE platform, Personal Data shared as part of document management, communication and administration of board work is processed. This may include, among other things:

Identification data (name, e-mail address, user name, position, and affiliation with the organisation)

Information contained in documents that are uploaded, processed or shared via the platform, including, for example, salary information, contract information, minutes of meetings, accounting material or other information about employees, management or business partners

Correspondence and activity data (e.g. comments, votes, meeting attendance)

Users may, at their own discretion – typically at the request of their organisation or board – upload identification documents such as a copy of a driving licence, passport or health insurance card. In such cases, a copy will only be made available to the board concerned, which is thereafter regarded as an independent data controller for the further processing of this information.

In addition to the Personal Data specified, further types of Personal Data may be processed depending on what the Customer chooses to share in its documents on the platform.

BOARD PEOPLE
In connection with the use of the BOARD PEOPLE platform, Personal Data that the data subject chooses to provide when creating and maintaining their profile is processed. This may include:

Identification data (name, contact details, title)

Profile information such as photo, presentation video, summary and personal CV

Information about personal and professional resources, background, education, board training, network and references

Information about current and previous board positions, professional experience, board experience and primary motivations for board work

4. The processing includes the following categories of data subjects

4.1 Management, board members and administrative staff, as well as other external stakeholders to whom the individual company grants access to the portal.

5. The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. Processing has the following duration

5.1 The personal data is processed until the termination of the personal data processing services, after which the personal data is deleted or returned in accordance with section 10. The processing is thus carried out for as long as the underlying commercial agreement(s) remain in force.

Appendix B Sub-processors

1. Approved sub-processors

1.1 On commencement of the Clauses, the Data Controller authorises the engagement of the following sub-processors:

The Data Processor's sub-processors are listed in the list of sub-processors in force at any given time, which can be accessed under the 'Security' tab on our website (https://www.board-office.dk/sikkerhed), or under 'Settings' within the individual portals.

1.2 On commencement of the Clauses, the Data Controller has authorised the use of the above-mentioned sub-processors for the processing activity described. The Data Processor shall not – without the Data Controller's written authorisation – engage a sub-processor for a processing activity other than the one described and agreed, or engage another sub-processor for this processing activity.

Appendix C Instruction pertaining to the processing of personal data

1. The subject of/instruction for the processing

1.1 The Data Processor processes personal data on behalf of the Data Controller in order to enable the Data Controller to use the board portal BOARD-OFFICE & BOARD-PEOPLE, which is an online portal containing document storage, a discussion forum, a planning tool, digital signature, board job listings and an inspiration area.

2. Security of processing

2.1 The level of security shall take into account:

The Data Processor shall establish an appropriate level of security taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Data Processor shall thereafter be entitled and obliged to decide which technical and organisational security measures are to be implemented to establish the necessary (and agreed) level of security.

The Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller:

Physical security

The Data Processor implements the following physical security measures:

a) The Data Processor's office premises can be locked.

b) The Data Processor has an alarm system to detect and prevent burglary.

c) The Data Processor has fire alarms and smoke detectors.

d) The Data Processor's equipment (including PCs, any servers etc.) is secured behind locked doors.

e) The Data Processor's buildings, premises and facilities or access routes are monitored (camera or video surveillance).

f) A control process or system is used to verify the identity of visitors.

g) The Data Processor uses key management, i.e. keys are issued to the relevant and necessary employees etc.

h) A log is kept of the Data Processor's visitors.

Organisational security

The Data Processor implements the following organisational security measures:

a) All employees are subject to a confidentiality obligation which applies to all personal data processed.

b) Employees' access to personal data in systems and on any physical media or facilities is restricted so that only the relevant employees have access to the relevant personal data.

c) Employees with access to personal data or critical IT systems are security-cleared prior to employment

d) Employees' processing of personal data is logged in whole or in part and can be checked as required.

e) The Data Processor has a documented process description for personal data breaches, which is reviewed at least once a year.

f) The Data Processor has an IT security policy.

g) The Data Processor has a fixed process which ensures that, in connection with repair, service and disposal of hardware, personal data on the hardware concerned is deleted or kept confidential.

h) The Data Processor's employees regularly document and report personal data breaches or risks thereof.

i) Employees with access to sensitive personal data (so-called 'sensitive' personal data) or critical IT systems are security-cleared prior to employment.

j) The Data Processor is able to take employment law measures in response to employees' breaches of the Data Processor's data security or breaches of instructions on the processing of personal data.

Home workstations shall be protected in the same way as workstations in the data processing facilities. Where an employee uses home/remote workstations, computers and other devices must never be left unattended without being locked or switched off. Two-factor authentication must be implemented to ensure that unauthorised persons cannot gain access to personal data. Access to the company's network resources, including access to systems, must take place via VPN.

The Data Processor ensures that all employees have been instructed in the relevant rules on, in particular, information security and data protection. The Data Processor shall furthermore ensure that all employees continuously receive awareness training on data security and thereby gain knowledge of how they should generally handle the processing of personal data, as well as the data protection risks associated therewith.

Technical security: Access to and protection of systems

The Data Processor implements the following technical security measures regarding access to and protection of systems:

a) The Data Processor's systems have logical access control by user name and password or other authorisation.

b) The Data Processor requires employees to use individual passwords.

c) The Data Processor's PCs have automatic access protection in case of inactivity, i.e. a locked screen saver.

d) The Data Processor uses anti-virus software which is updated regularly.

e) A policy for the composition of passwords is applied, including minimum requirements.

f) There are procedure(s) for revoking permissions when an employee leaves the Data Processor or changes department.

g) Unauthorised or repeated failed attempts to log in to the Data Processor's systems are logged and monitored.

h) There are procedure(s) for granting authorisations to IT systems when an employee is hired.

Automatic daily backup of the database, via the storage and backup solution IBM Tivoli Storage Manager.

Personal data is encrypted in systems and/or on storage media where relevant and taking into account the processing and the nature of the personal data.

Firewall, which is updated continuously in order to maintain complete protection.

Anti-virus software, which is updated continuously to ensure that both the program's modules and the system components can maintain complete protection.

The Data Processor's websites use HTTPS (Hyper Text Transfer Protocol Secure), so that all communication on the open internet is encrypted peer-to-peer.

The Data Processor is obliged, on an ongoing basis and within a reasonable time, to use tools for vulnerability scanning and subsequently apply security updates to all devices and systems from which personal data is accessed.

Two-factor authentication (two-factor login) is used as a technical security measure when logging in to the BOARD OFFICE and BOARD PEOPLE systems to ensure that only authorised users gain access to personal data and other data.

Technical security: Access to personal data (data)

The Data Processor implements the following technical security measures regarding access to personal data:

a) The Data Processor regularly reviews and checks user authorisations for specific systems.

b) The Data Processor has traceability of access to, modification of and deletion of data by individual users.

c) The Data Processor grants individual users or groups of users authorisations to access, modify and delete processed personal data.

d) The Data Processor has procedure(s) for restoring/re-establishing data from backup.

e) The Data Processor logs and monitors unauthorised or repeated failed attempts to access data.

f) The Data Processor regularly reviews system controls.

Technical security: Encryption

The Data Processor implements the following technical security measures regarding encryption:

a) Content on external hard drives and USB keys etc. is encrypted when these media contain personal data or sensitive personal data.

b) The Data Processor's websites use HTTPS (Hyper Text Transfer Protocol Secure).

c) The Data Processor's computers have encrypted hard drives.

d) Personal data is encrypted in relevant systems and/or on storage media.

e) Passwords stored on the Data Processor's computers etc. are encrypted.

f) Sensitive personal data is encrypted in systems and/or on storage media.

g) Network encryption is used.

Technical security: Control of transmission

The Data Processor implements the following technical security measures regarding control of transmission:

a) The Data Processor uses and has guidelines for secure e-mail.

b) Outgoing e-mails containing sensitive personal data or information about purely private matters are encrypted.

c) Guidelines for the use of work e-mail, including private use, appropriate use, encryption, secure use etc.

The Data Processor ensures that the TLS encryption used always complies with the latest applicable minimum standards.

Technical security: Availability and resilience

The Data Processor implements the following technical security measures regarding availability and resilience:

a) Availability and resilience of the Data Processor's systems and servers are ensured by a third party with whom the Data Processor has an agreement.

b) Only authorised employees have access to any of the Data Processor's own servers.

c) Server rooms have smoke alarms and fire extinguishers.

d) Server rooms have an air-conditioning system.

e) There are rules and guidelines for backup of data.

f) There are rules and guidelines for restoring data from backup.

g) Regular backups are performed (either in-house or at a supplier).

h) Active alerts in case of attempted unauthorised access to server rooms and/or processing systems and data.

i) An uninterruptible power supply (UPS) is used.

j) Temperature and humidity are monitored in server rooms.

k) The Data Processor has procedure description(s) for personal data breaches, which are reviewed at least once a year.

3. Assistance to the data controller

3.1 The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clauses 8.1 and 8.2 by implementing the following technical and organisational measures:

3.1.1 If the Data Controller receives a request for the exercise of individuals' rights under applicable data protection legislation, and a correct response to the request requires assistance from the Data Processor, the Data Processor shall assist the Data Controller with necessary and relevant information and documentation as well as appropriate technical and organisational security measures.

3.1.2 If the Data Controller wishes to receive assistance in responding to a request from a data subject, the Data Controller shall send a written request to that effect to the Data Processor, and the Data Processor shall in response provide the necessary assistance or documentation as soon as possible and no later than 7 calendar days after receipt of the request.

3.1.3 If the Data Processor receives a request for the exercise of individuals' rights under applicable data protection legislation from anyone other than the Data Controller, and the request concerns personal data processed on behalf of the Data Controller, the Data Processor shall forward the request to the Data Controller without undue delay.

4. Storage period/erasure procedures

4.1 Upon termination of the licence agreement, data is stored for a period of 12 months after termination, after which the board and all associated data are automatically deleted without further notice to the Customer. The Customer may, however, request earlier deletion, after which the Data Processor will carry out manual deletion within a reasonable time. Deletion is carried out in a manner that ensures that the information cannot be restored or reconstructed, in accordance with the Data Processor's security procedures and applicable data protection legislation.

As regards the individual user profile, the associated personal data is deleted upon written request from the Customer to the Data Processor (BOARD OFFICE A/S).
Upon receipt of such a request, the Data Processor carries out manual deletion of the user profile concerned and all associated information without undue delay and in accordance with the Data Processor's internal procedures for secure deletion. The Customer receives written confirmation of completed deletion when the process has been completed. User profiles are automatically deactivated after 4 years of inactivity (since last login) and automatically deleted 1 year after deactivation.

5. Processing location

5.1 Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

At the Data Processor's own head offices and at the head offices of approved sub-processors, as set out in Appendix B.

6. Instruction on the transfer of personal data to third countries

6.1 The personal data is only processed by the Data Processor at the locations described in Clause C.5. Transfers to the USA take place on the basis of the data importer's certification under the EU-U.S. Data Privacy Framework (see certified organisations here.)

6.2 If the Data Controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Clauses to perform such transfers.

6.3 Transfer of personal data may in all cases only take place as prescribed in the Clauses, on the Data Controller's instructions, and to the extent permitted under data protection legislation.

6.4 Where the transfer of the personal data to third countries outside the EU/EEA takes place through the Data Processor's transfer to sub-processors, the Data Controller hereby authorises the Data Processor, on behalf of the Data Controller, to enter into the standard contractual clauses adopted by the Commission with the Data Processor's sub-processors, provided that all rules of data protection legislation on transfer and processing are otherwise complied with. Where the Data Controller is itself a data processor, and the Data Processor acts as sub-processor for the personal data in relation to the Data Controller's ultimate contracting party(ies), the Data Controller shall obtain authorisation from the ultimate contracting party for the Data Processor to enter into the standard contractual clauses.

6.5 Where the Data Processor, in accordance with these clauses, transfers personal data covered by the agreement onwards to sub-processors or independent data controllers in third countries, the Data Processor shall itself ensure that the transfer complies with Chapter 5 of Regulation 2016/679.

7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

7.1 The Data Processor shall, upon written request, document to the Data Controller that the Data Processor

7.1.1 complies with its obligations under this Data Processing Agreement and the Instruction, and

7.1.2 complies with the provisions of the GDPR as regards the personal data processed on behalf of the Data Controller.

7.2 The Data Processor's documentation pursuant to section C.7.1 shall be sent to the Data Controller within a reasonable time after receipt of the request.

7.3 As documentation of ongoing compliance with the Clauses, the Data Processor shall make self-assessment reports available to the Data Controller. These self-assessment reports shall be prepared at least once a year and shall follow the principles and control objectives of the auditing standard ISAE 3000 as prepared by FSR – Danish Auditors and the Danish Data Protection Agency (Datatilsynet) (and/or alternatively other internationally recognised standards such as ISO/IEC 27701:2019). At the Data Controller's option, the self-assessment reports may be carried out through the Data Controller's collection of information and shall be signed by the Data Processor's management. The Data Processor is not obliged itself to initiate and carry out an external audit of the Data Processor's compliance with the Clauses.

7.4 Notwithstanding section C.7.3, the Data Processor shall furthermore allow for and contribute to audits and inspections every 12 months, carried out by auditors appointed by the Data Controller, the public authorities in Denmark or of another competent jurisdiction, to the extent necessary to verify that the Data Processor complies with the Clauses and applicable data protection legislation. The auditor concerned shall be subject to confidentiality by law or agreement. The Data Controller shall give 10 calendar days' written notice of audits as described.

8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

8.1 The Data Processor supervises sub-processors annually by obtaining the sub-processor's own reports, management statements or similar, certifications or an auditor's report from an independent third party concerning the sub-processor's compliance with the General Data Protection Regulation, the data protection provisions of other EU law or the national law of the Member States and these Clauses.

The parties agree that the following types of certifications and auditor's reports may be used in accordance with these clauses:
ISAE 3000
ISAE 3402
ISO 27001
ISO 27701
SOC2

The Data Processor shall be able to document to the data controller that the supervision has taken place.

Based on the results of the supervision, the data processor (and the data controller) is entitled to request the implementation of additional measures to ensure compliance with the General Data Protection Regulation, the data protection provisions of other EU law or the national law of the Member States and these Clauses.

If the sub-processor is unable to meet the additional measures required on the basis of the supervision, the data processor is obliged to examine the possibility of replacing the sub-processor.

The Data Processor or a representative of the Data Processor is furthermore entitled to carry out inspections, including physical inspections, of the locations from which the sub-processor processes personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the data processor (or the data controller) deems it necessary.

Documentation of such inspections shall be sent to the data controller without undue delay if the supervision reveals that a sub-processor is not considered to be in compliance with applicable requirements. In such cases, the data controller may contest the framework and/or the method of the inspection and request that a new inspection be carried out under a different framework and/or using a different method.

Any expenses of the Data Processor and the sub-processor in connection with a physical inspection of the sub-processor's locations shall not be charged to the data controller – regardless of whether

the data controller has initiated and participated in such an inspection.

Appendix D The Parties' terms of agreement on other subjects

1. Other matters

1.1 The Data Processing Agreement does not regulate other matters.

Appendix E – Processing of personal data when using BOARD Assistant™

This appendix describes the Data Processor's processing of personal data in connection with customers' and users' use of BOARD Assistant™ ("the AI functionality") in the BOARD OFFICE™ and BOARD PEOPLE™ portals.

The appendix forms an integral part of the Data Processing Agreement and specifies the purpose, data flow, processing activities, security measures, use of sub-processors and the conditions for the customer's choice of functionality, including the use of secure mode versus real-time search.

1. Purpose of the processing

1.1. The purpose of BOARD Assistant™ is to give users access to AI-supported functions that can support board work, document comprehension, summaries, template assistance, draft agendas, knowledge search etc., all in a private, encrypted and isolated environment where data does not leave the EU.

1.2. BOARD Assistant™ uses Microsoft Azure OpenAI in EU data centres.

1.3. BOARD Assistant™ is designed so that input data is not stored, not used for training, not logged outside the BOARD OFFICE platform and not shared with other customers.

2. Nature of the processing and data categories

2.1. BOARD Assistant™ only processes the data that the user actively enters in the chat or the AI function, as well as the documents or text excerpts that the user chooses to send for AI analysis.

2.2. Typically, the following personal data may be processed:

- Identification data included in board documents (name, title etc.)
- Information in documents uploaded to BOARD OFFICE (e.g. contracts, minutes, accounts, CVs etc.)
- Information from BOARD PEOPLE profiles if the user activates AI functions in BOARD PEOPLE
- Any other personal data that the user includes in their interaction with the AI function

2.3. BOARD Assistant™ does not carry out any automated decision-making or profiling that has legal or similarly significant consequences for individuals.

3. Technology, operation and data storage

3.1. BOARD Assistant™ uses Azure OpenAI EU Standard Zone, where:

- All processing takes place within EU data centres
- Microsoft does not use customer data for training
- There is no logging or external lookup of input data
- Data is only processed transiently (not stored) in the AI engine

3.2. BOARD OFFICE only stores the data that the user chooses to save in the platform – AI input and AI results are not stored by Azure, and only by BOARD OFFICE if the user actively saves the content.

3.3. All communication between BOARD OFFICE and Azure OpenAI takes place via encrypted connections (TLS 1.2+) and via private endpoints.

4. Separation between the operating environment and real-time search

4.1. BOARD Assistant™ is delivered by default in a secure mode, where:

- No data leaves BOARD OFFICE or the Azure EU zone
- No searches are made in external sources or on the internet
- No real-time information is retrieved
- No processing ever takes place outside the EU/EEA

4.2. If the user activates the real-time search function:

- The user must actively opt in to the function
- The user receives an explicit warning that data may thereafter be processed outside the isolated environment
- Processing may take place outside the EU, depending on Microsoft's processing of search queries
- This function is regarded as an independent data processing choice which serves as an instruction from the Data Controller

4.3. BOARD OFFICE logs the user's choice, but never logs the content of the individual queries.

5. Sub-processors

5.1. BOARD Assistant™ uses the following sub-processor:

- Microsoft Azure (EU data centres) – AI functionality

5.2. No further sub-processors are used for the AI functionality.

5.3. When real-time search is activated, Microsoft's Bing infrastructure may be regarded as an additional processing chain – this use is only triggered by the Data Controller's/user's active instruction.

6. Transfer to third countries

6.1. In secure mode, all personal data is processed exclusively within the EU/EEA in Azure EU data centres.

6.2. When real-time search is used, transfers to third countries only take place if the user actively chooses the function.

6.3. The Data Controller's activation of real-time search is regarded as a documented instruction regarding third-country transfer.

7. Security measures

7.1. BOARD Assistant™ is covered by the technical and organisational measures already described in Appendix C.

7.2. Specific AI-related security measures include:

- Use of private endpoints between BOARD OFFICE and Azure OpenAI
- Zero-data retention
- Encryption of all queries and responses in transit
- Model isolation, so that data from one customer can never be accessed by others
- No training, no cache, no persistent storage in the AI environment

8. Assistance to the Data Controller

8.1. BOARD OFFICE assists the Data Controller in accordance with the data processing agreement.

8.2. BOARD OFFICE can document:

- Whether a user has used secure mode or real-time search
- Whether a user has saved AI-generated content in the portal
- Relevant security logs regarding access and system operation

8.3. BOARD OFFICE cannot reconstruct AI queries, as these are not stored.

9. Erasure

9.1. As BOARD Assistant™ does not itself store personal data, there are no separate erasure rules.

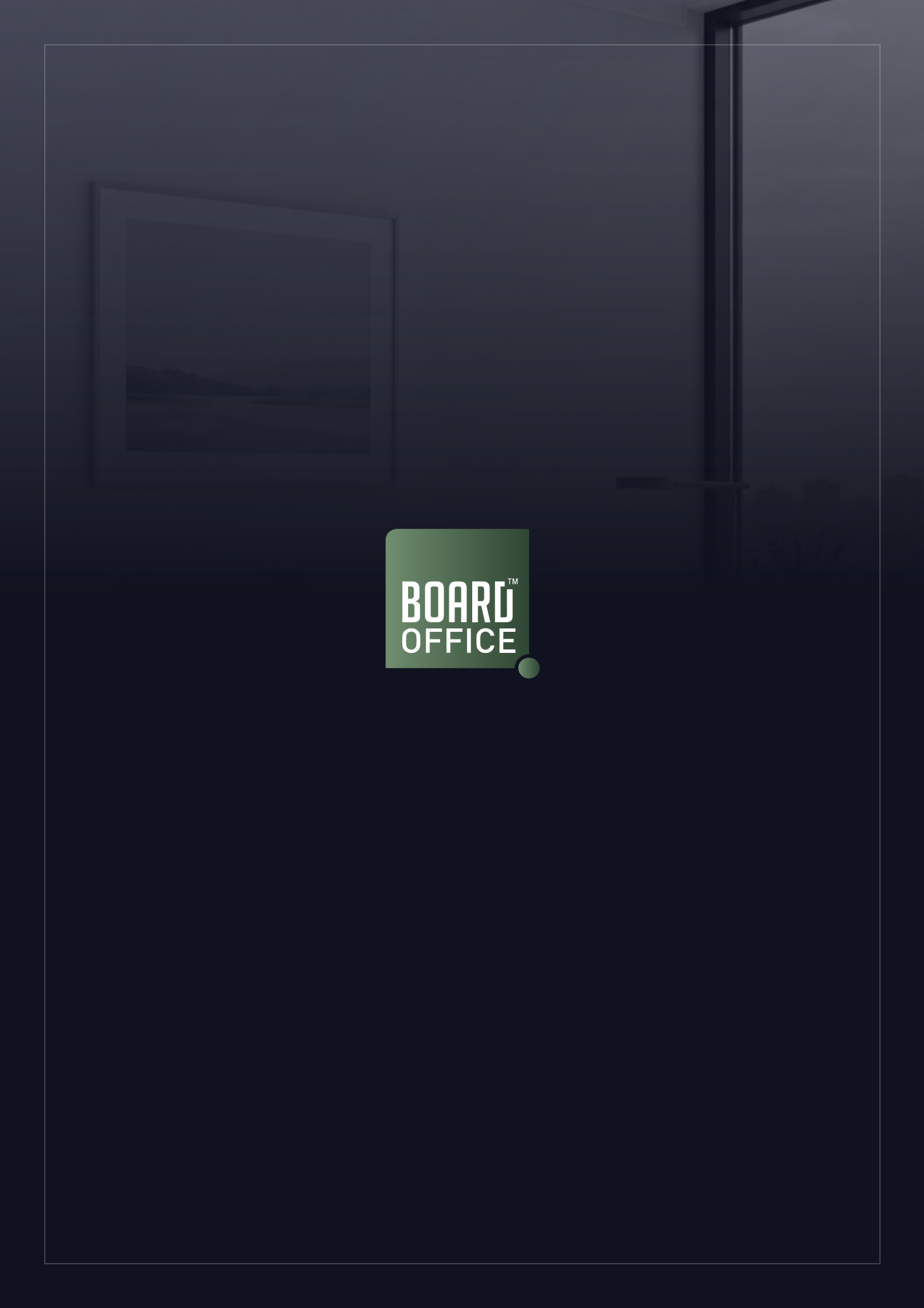
9.2. AI-generated content saved in BOARD OFFICE is processed in accordance with the general erasure rules of the data processing agreement.

10. Changes to instructions

10.1. The Data Controller may at any time choose to:

- Deactivate BOARD Assistant™
- Restrict to secure mode
- Allow or refuse the use of real-time search
- Set up internal policies for its use

10.2. Changes are documented in the customer's settings and serve as instructions.


BOARD™
OFFICE